AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions of claims in the application:

1. (Canceled)

2. (Currently Amended) A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

~~The method of claim 1, wherein said filtering further comprises:~~

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, said filtering including:

updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count;

and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

3. (Original) The method of claim 2, wherein said applying further comprises setting an alarm when said request count exceeds said maximum HTTP request count.

4. (Original) The method of claim 3, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

5. (Original) The method of claim 2, wherein said applying further comprises dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

6. (Original) The method of claim 2, wherein said applying further comprises shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

7. (Original) The method of claim 6, wherein said applying further comprises disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

8. (Original) The method of claim 7, further comprising increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

9. (Original) The method of claim 8, wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

10. (Canceled)

11. (Currently Amended) A method for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

~~The method of claim 1,~~

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, wherein said filtering ~~further~~ comprises indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency; and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

12. (Canceled)

13. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to prevent denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

~~The program storage device of claim 12, wherein said filtering further comprises:~~

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, said filtering including:

updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count;

and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

14. (Original) The program storage device of claim 13, wherein said applying further comprises setting an alarm when said request count exceeds said maximum HTTP request count.

15. (Original) The program storage device of claim 14, further comprising sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

16. (Original) The program storage device of claim 13, wherein said applying further comprises dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

17 (Original) The program storage device of claim 13, wherein said applying further comprises shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

18. (Original) The program storage device of claim 17, wherein said applying further comprises disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

19. (Original) The program storage device of claim 18, further comprising increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

20. (Original) The program storage device of claim 19, wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

21. (Canceled)

22. (Currently Amended) A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to prevent denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the method comprising:

~~The program storage device of claim 12,~~

receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

receiving a profile for said subscriber;

filtering said request to determine whether said subscriber is authorized to make said request based upon said profile, wherein said filtering ~~further~~ comprises indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency; and

forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

23. (Canceled)

24. (Currently Amended) An apparatus for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the apparatus comprising:

~~The apparatus of claim 23, wherein said means for filtering further comprises:~~

means for receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

means for receiving a profile for said subscriber;

means for filtering to determine whether said subscriber is authorized to make said request based upon said profile, said means for filtering including:

means for updating a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

means for applying HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count;

and

means for forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

25. (Original) The apparatus of claim 24, wherein said means for applying further comprises means for setting an alarm when said request count exceeds said maximum HTTP request count.

26. (Original) The apparatus of claim 25, further comprising means for sending said alarm to an Internet Service Provider (ISP) associated with said subscriber.

27. (Original) The apparatus of claim 24, wherein said means for applying further comprises means for dropping the data packet containing said request when said request count exceeds said maximum HTTP request count.

28. (Original) The apparatus of claim 24, wherein said means for applying further comprises means for shutting down the account used to access said first communication network when said request count exceeds said maximum HTTP request count.

29. (Original) The apparatus of claim 28, wherein said means for applying further comprises means for disabling HTTP requests for a hold-down period when said request count exceeds said maximum HTTP request count.

30. (Original) The apparatus of claim 29, further comprising means for increasing said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

31. (Original) The apparatus of claim 30, wherein said hold-down period increases exponentially each time said HTTP count exceeds said maximum HTTP request count.

32. (Canceled)

33. (Currently Amended) An apparatus for preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, the apparatus comprising:

~~The apparatus of claim 23,~~

means for receiving a HTTP request from a subscriber using a first communication network coupled to at least one other communication network, said request including a Universal Resource Locator (URL);

means for receiving a profile for said subscriber;

means for filtering to determine whether said subscriber is authorized to make said request based upon said profile, wherein said filtering ~~further~~ comprises means for indicating said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency; and

means for forwarding said request to said at least one other communication network when said subscriber is authorized to make said request.

34, 35. (Canceled)

36. (Currently Amended) An apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, said apparatus comprising:

~~The apparatus of claim 35, wherein said filter further comprises:~~

a first receiving interface capable of accepting a HTTP request received from a subscriber using a first communication network, said request including a Universal Resource Locator (URL);

a profile request generator capable of generating a profile request based upon said request;

a first forwarding interface capable of sending said profile request to an AAA server;

a second receiving interface capable of accepting a requested profile;

a filter capable of determining whether said request is authorized based upon said requested profile, said filter including:

an updater to update a client HTTP request count when said request is a HTTP "GET" request or a HTTP "POST" request; and

a responder to apply HTTP server attack preventative measures when said request count exceeds a maximum HTTP request count;

an authorizer capable of allowing said request to be forwarded on at least one other communication network coupled to said first communication network; and

a second forwarding interface capable of forwarding said request on said at least one other communication network.

37. (Original) The apparatus of claim 36, wherein said responder further sets an alarm when said request count exceeds a maximum HTTP request count.

38. (Original) The apparatus of claim 36, wherein said responder sends said alarm to an Internet Service Provider (ISP) associated with said subscriber.

39. (Original) The apparatus of claim 36, wherein said responder drops the data packet containing said request when said request count exceeds a maximum HTTP request count.

40. (Original) The apparatus of claim 36, wherein said responder shuts down the account used to access said first communication network when said request count exceeds a maximum HTTP request count.

41. (Original) The apparatus of claim 40, wherein said responder disables HTTP requests for a hold-down period when said request count exceeds a maximum HTTP request count.

42. (Original) The apparatus of claim 41, wherein said responder increases said hold-down period each time said HTTP count exceeds said maximum HTTP request count.

43. (Original) The apparatus of claim 42, wherein said responder increases said hold-down period exponentially each time said HTTP count exceeds said maximum HTTP request count.

44. (Canceled)

45. (Currently Amended) An apparatus capable of preventing denial of service attacks against Hypertext Transfer Protocol (HTTP) servers, said apparatus comprising:

~~The apparatus of claim 34,~~

a first receiving interface capable of accepting a HTTP request received from a subscriber using a first communication network, said request including a Universal Resource Locator (URL);

a profile request generator capable of generating a profile request based upon said request;

a first forwarding interface capable of sending said profile request to an AAA server;

a second receiving interface capable of accepting a requested profile;

a filter capable of determining whether said request is authorized based upon said requested profile, wherein said filter indicates said request is unauthorized when the frequency of HTTP requests for said URL exceeds a maximum HTTP request frequency;

an authorizer capable of allowing said request to be forwarded on at least one other communication network coupled to said first communication network; and

a second forwarding interface capable of forwarding said request on said at least one other communication network.